UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/612,715	07/01/2003	Luz Maria Soto	010942-0304513 AUD-001(U)	3762

7590 02/26/2007

Pillsbury Winthrop LLP
Intellectual Property Group
1600 Tysons Boulevard
McLean, VA 22102

EXAMINER	
SHAN, APRIL YING	
ART UNIT	**PAPER NUMBER**
2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/612,715	SOTO ET AL.	
	Examiner	Art Unit	
	April Y. Shan	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 November 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. The Applicant's Supplement Amendment, filed 29 November 2006, has been received, and respectfully and carefully considered.

2. As a result of the amendment, claims 1, 2, 14, 15, 27 and 28 have been amended. Claims 1-28 are now presented for examination.

3. Examiner is aware of the Supplement Amendment and it will replace the previous responsive amendment filed 21 November 2006.

Claim Objections

4. Examiner carefully and fully reviewed the Applicant's argument on page 7 about withdrawing the claim objections for claims 6 and 19. They are not persuasive. It is true that the Applicant can claim broadly in the claims. But for claims 6 and 19, the Applicants expressly narrow the term "key administrator" in claims 6 and 19 by the claim limitations **"...the key administrator being a person different than the key generators".**

Examiner carefully and fully reviewed the Applicant's original disclosure and found on page 18, the Applicant discloses "administrator". Therefore, the examiner decides to withdraw the claim objections for claims 6 and 19.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> **The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the**

art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claims 1-28 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

The Applicant amended the independent claims 1, 14 and 27 by adding new claim limitations, "if a result of the comparing step indicates a match: encrypting the request with a private key, **wherein the private key is not provided to the user**, and providing the service with access to a public key corresponding to the private key" and "the server encrypts the requests with a private key..."

The examiner carefully and fully reviewed the original disclosure and respectfully points out on page 10, lines 1-3 and 5-9 of the original disclosure, the Applicant discloses "...the user's private key...and only accessed after a valid biometric signature 208 has been authenticated...An authorized user...encrypted using his/her private key 206", on page11, lines 14-16 of the original disclosure, the Applicant discloses " "Biometric comparison is thereafter done against the registered template for an individual **in order to grant access to the individual's private key 206** for a transaction" and in page 13, lines 1-4 of the original disclosure, the Applicant discloses "If the biometric signature submitted by the individual in conjunction with the request for a digital signature does not match...the individual's private key 206 is not access and/or used for the request." **In fact, the new limitation is not only a new limitation not**

supported by the original disclosure, but also a new claim limitation contradicted to the original disclosure and also it is wrong. According to Applicant's original disclosure, the private key is not provided **by** the user, but if the biometric sample matches to the biometric template associated with the user, the private key is accessed and/or used for the request. Therefore, the private key is provided to the user to encrypt the request according to Applicant's disclosure. Also, the new claim limitation "the server encrypts the requests with a private key" in claim 27 defeated the purpose of security and completely contradicted to Applicant's original disclosure. From this new limitation, a client sends a plain request without encryption to a server, thus the request is not protected at all during the transmission from the client to the server. Then the server encrypts the request with a private key, it is too late since the request is already captured by the third party in plain format on the way from the client to the server. Therefore, the original disclosure discloses that the private key is not provided by the user and therefore, the user does not have to carry a smart card. After the verification, the server provides the private key to the user and therefore user encrypts the request before sending to the server (Please see fig. 3 and 4).

The Applicant amended dependent claims 2 and 15 by adding new claim limitations "**and sending the generated digital signature to the user**".

The examiner carefully and fully reviewed the original disclosure and respectfully points out on page 16, lines 19-21 of the original disclosure, the Applicant discloses "The digital signature associated with the transaction...is then forwarded downstream for processing by the receipt" and on page 21, lines 14-15, the Applicant discloses "The

digital signature is then appended to the message to the service/receipt". According to claim 1, a user is the sender and the service is the receipt. The original disclosure has no support that the generated digital signature to the user (sender), but to the service (receipt). The limitation is not an original limitation; it was added by an amendment not supported by the original disclosure.

"When filling an amendment an applicant should show support in the original disclosure for new or amended claims." M.P.EP. § 2163.II.A.3 (b).

Any claim not specifically addressed, above, is being rejected as incorporating the deficiencies of a claim upon which it depends.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1-5, 9-18 and 22-28 are rejected under 35 U.S.C. 102(e) as being anticipated by Gould et al. (U.S. Patent 6,920,561).

As per **claim 1**, Gould et al. discloses a method comprising:

a method comprising:

receiving a request for access to a service ("Biometric input and user credentials are associated together to provide a template which is stored in a database on the

server..." – e.g. col. 5, lines 2-7. Please note user credentials corresponds to Applicant's request);

collecting a biometric sample from a user associated with the request (e.g. col. 5, lines 2-7, col. 5, lines 14-17 and step 402 in fig. 4);

comparing the biometric sample to a biometric template associated with the user (e.g. col. 5, lines 26-28 and step 412 of fig 4); and if a result of the comparing step indicates a match (e.g. step 412 of fig. 4 and col. 5, lines 26-31): encrypting the request with a private key (e.g. col. 5, lines 33-35), wherein the private key is not provided to the user (e.g. col. 5, lines 34-35. Please note the private key is the server private key. Therefore, it is not provided to the user), and providing the service with access to a public key corresponding to the private key (e.g. col. 5, lines 39-41 and fig. 420. Please note client is the service and client has access to server's public key).

As per **claims 2, 4, 9, 12**, Gould et al. discloses a method as applied in claim 1. Gould et al. further discloses if the result indicates a match, generating a digital signature using the private key and sending the generated digital signature to the user (e.g. steps 418-426 and col. 5, lines 35-45, "User has full use of credentials during session and is enabled for all certificate and signature functions"), providing a biometric signature corresponding to the collected biometric sample to the service associated with the request (col. 1, lines 54-55 and col. 1, lines 63-67 – col. 2, lines 1-3, steps 406 and 408 in fig. 4), encrypting the collected biometric sample for transmission to an authentication server (col. 5, lines 19-21 and claim 1/b and claim 6); and including

integrity information in the encrypted biometric sample (col. 5, lines 19-21, steps 406 and 408 in fig. 4); associating user identification information with the private key (col. 5, lines 32-36 and step 416 in fig. 4); and maintaining a digital certificate containing the user identification information and a public key corresponding to the private key (col. 5, lines 32-47).

As per **claim 3**, Gould et al. discloses a method as applied in claim 2. Gould et al. further discloses providing the digital signature to the service associated with the request (e.g. step 406 of fig.4, steps 418-426 and col. 5, lines 35-46).

As per **claim 5**, Gould et al. discloses a method as applied in claim 4. Gould et al. further discloses allowing the service to determine whether to fulfill a transaction corresponding to the request in accordance with the result of the comparing step (step 420, 422, 424 and 426 of fig. 4).

As per **claims 10 and 11**, Gould et al. discloses a method as applied in claim 9. Gould et al. further discloses decrypting the encrypted biometric sample at the authentication server (col. 5, lines 22-26); and checking the integrity information included with the biometric sample (step 410 of fig. 4) and wherein the integrity information includes a unique transaction identifier (signature and message via step 410 of fig. 4 – e.g. col. 5, lines 25-26).

As per **claim 13**, Gould et al. discloses a method as applied in claim 1. Gould et al. further discloses wherein the biometric sample includes a fingerprint scan (col. 4, lines 41-44).

As per **claim 14**, it is rejected using the same rationale as for rejecting claim 1.

As per **claim 15**, it is rejected using the same rationale as for rejecting claim 2.

As per claims **17, 22 and 25**, Gould et al. discloses an apparatus as applied in claim 14. Gould et al. further discloses means for providing a biometric signature corresponding to the collected biometric sample to the service associated with the request (col. 1, lines 54-55 and col. 1, lines 63-67 – col. 2, lines 1-3), means for encrypting the collected biometric sample for transmission to an authentication server (col. 5, lines 19-22 and claims 7 and 13); and means for including integrity information in the encrypted biometric sample (col. 5, lines 19-21) and means for associating user identification information with the private key (col. 5, lines 32-36 and step 416 in fig. 4); and means for maintaining a digital certificate containing the user identification information and a public key corresponding to the private key (col. 5, lines 32-47).

As per **claim 16**, Gould et al. discloses an apparatus as applied in claim 15. Gould et al. further discloses means for providing the digital signature to the service associated with the request (step 406 of fig.4, steps 418-426 and col. 5, lines 35-46).

As per **claim 18**, Gould et al. discloses an apparatus as applied in claim 17.

Gould et al. further discloses means for allowing the service to determine whether to fulfill a transaction corresponding to the request in accordance with a result of the comparing means (col. 5, lines 38-46).

As per **claims 23 and 24**, Gould et al. discloses an apparatus as applied in claim 22. Gould et al. further discloses means for decrypting the encrypted biometric sample at the authentication server (col. 5, lines 22-26); and means for checking the integrity information included with the biometric sample (step 410 of fig. 4) and wherein the integrity information includes a unique transaction identifier (signature and message via step 410 of fig. 4 – e.g. col. 5, lines 25-26).

As per **claim 26**, Gould et al. discloses an apparatus as applied in claim 14. Gould et al. further discloses wherein the biometric sample includes a fingerprint scan (col. 4, lines 41-44).

As per **claim 27**, it is rejected using the same rationale as rejecting claim 1.

As per **claim 28**, Gould et al. discloses an authentication infrastructure as applied in claim 27. Gould et al. further discloses wherein the private key is used to sign a message (col. 5, lines 35-37) for allowing the user to perform the transaction with the service, the service obtaining a corresponding public key from the server (col. 5, lines 38-40).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

11. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

12. Claims 6-8 and 19-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gould et al. (cited above)

As per **claims 6-8 and 19-21**, Gould et al. show the method, apparatus and authentication infrastructure discussed above in claims 1-5, 9-18 and 22-28. Gould et al. further teaches creating the biometric template for the user only if registration is verified (col. 5, lines 2-4 and see below response to arguments) and generating the private key only if the biometric template is successfully created (col. 5, lines 19-64 and abstract "The user can then have their individual credentials securely imported to the local client for subsequent use...without needing any additional identification or memory token such as a smart card"). Gould et al. does not specifically show generating pre-enrollment keys and final pre-enrollment key from different individuals. The Examiner takes Official Notice that one of ordinary skill in the art would know generating pre-enrollment keys and final enrollment key from different individuals in the process of enrollment of a user (A department store central server grants a customer random generated codes (these codes are pre-enrollment keys) showing on a receipt to the customer upon verifying/keying the customer's credential by a store's salesman during store credit card enrollment, which allows the customer to shop for a set of time period until the real store credit card arrives. A different operator at the card-issuing office verifies the information and grant/mail the customer an official store credit card. The code on the official card is the final enrollment key). Therefore, it would be obvious to one of ordinary skill in the art at the time of the invention to add this feature motivating by providing convenience and security to the customer.

Double Patenting

13. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

14. Claims 1, 13, 14, 26 and 27 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 17, 18, 20, 36, 39 and 44 of copending Application No. 09/801,468 (U.S. Patent Application Publication 2003/0208684). Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1, 17, 18, 20, 36, 39 and 44 in the copending application encompass the same subject matter as claims 1, 13, 14, 26 and 27 in the application. This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim 1 recites a method comprising: receiving a request for access to a service (claim 1, "receiving a message ...to use on-line resources" of copending

application publication); collecting a biometric sample from a user associated with the request (claim 1, "obtaining an indicia of physical identification... if authentication is required" of copending application publication and claim 17, "wherein the indicia is a biometric" in the copending application publication); comparing the biometric sample to a biometric template associated with the user (claim 1, "comparing the obtained indicia...for the user" of copending application publication); and providing access to a private key in accordance with a result of the comparing step (claim 1, "enabling the request...matches the stored indicia" of copending application publication).

Claim 13 recites wherein the biometric sample includes a fingerprint scan (claim 18, "wherein the biometric is one or more a fingerprint....and a handwriting sample" of copending application publication).

Claim 14 recites an apparatus comprising: means for receiving a request for access to a service (claim 20, "means for receiving a message...to use on-line resources" of copending application); means for collecting a biometric sample from a user associated with the request (claim 20, "means for obtaining an indicia of physical identification...if authentication is required" of copending application and claim 36, "wherein the indicia is a biometric" of copending application); means for comparing the biometric sample to a biometric template associated with the user (claim 20, "means for comparing the obtained indicia...for the user"

of copending application); and means for providing access to a private key in accordance with a result of the comparing step (claim 20, "means for enabling the request...matches the stored indicia" of copending application publication).

Claim 26 recites wherein the biometric sample includes a fingerprint scan (claim 37, "wherein the biometric is one or more of a fingerprint....and a handwriting sample" of copending application).

Claim 27 recites an authentication infrastructure comprising: a server that intercepts requests for access to a service (claim 39, "a server that is adapted to communicate...to use the network based service" of copending application); and a client that collects a biometric sample from a user associated with the request (claim 39, "a rule subsystem...if authentication is required" of copending application and claim 44, "wherein the indicia is a biometric" of copending application), wherein the server maintains a biometric template associated with the user for authenticating the collected biometric sample (claim 39, "an authentication subsystem...to a stored indicia for the user" of copending application), and wherein the server provides access to a private key in accordance with a result of the authentication, so that the user need not maintain a token for accessing the service.

Response to the Argument

15. Applicant's arguments filed 29 November 2006 have been fully considered but they are not persuasive.

16. Applicant's argument over Objections to the claims on page 7 has been addressed above.

17. Applicant's arguments over amended independent claims 1, 4 and 27 on page 8 have been addressed in the above 35 USC § 112 rejection and new ground rejection using the Gould et al. reference. Further, the examiner disagrees with Applicant's statement that "Each client computer already has its own unique private key that is automatically provided to the user (col. 5, lines 19-21)". The examiner respectfully points out that client and user are two different entities according to the Gould et al. reference. According to fig. 1, a client is part of the system, which can be a computer and user is a human user according to the abstract. Please read closely in col. 5, lines 19-21, "**The client** 104 then signs and encrypts this template using the client unique platform private key....". It clearly states that the client encrypts the template, not the user. Therefore, Applicant's interpretation on Gould et al. reference that "the private key is automatically provided to the user" is completely wrong. Furthermore, the Applicant's statement "clearly, the user of Gould's system does not need to do anything to get access to the private key apart from sitting at the computer" is contradicted to the new limitations the Applicant added to independent claims 1, 14 and 27 "wherein the private key is not provided to the user" and "the server encrypts the request with a private key....". Again, the Applicant's own statement agrees with the examiner that Gould et

al. reference teaches the new limitation added by the Applicant that "private key is not provided to the user".

18. Applicant's argument over amended dependent claims 2 and 15 have been addressed in the above 35 USC § 112 rejection and new ground rejection using the Gould et al. reference.

19. Applicant's arguments over claims 3-4 and 16-17 on page 9 are not persuasive and the examiner disagrees. Examiner respectfully points out Applicant misunderstands the Gould et al. reference. In the Gould et al. reference, user requests service from the client computer and therefore, the client computer is the service/receipt. Please see fig. 4 and abstract, "....The user can then have their individual credentials securely imported to the local client for subsequent use during that time period,..."

20. Applicant's argument over claims 9 and 22 are not persuasive and the examiner disagrees. Examiner respectfully points out in steps 406 and 408 in fig. 4, Gould et al. clearly discloses "Client encrypts and **signs** this template using the client unique platform private key and Client sends this data to Authentication/Credential Server)

21. Applicant's argument over claims 10 and 23 are not persuasive and the examiner disagrees. Examiner respectfully points out in steps 410, 412 and 414 in fig. 4, Gould et al. clearly discloses "Authentication/Credential Server verifies data is from an authorized client in its enterprise by using client platform public key to verify the signature and message, server uses the verified and decrypted biometric data and matches against previously enrolled templates and server pulls from a secure database the appropriate

authentication credentials for the biometric identified user". To a person with ordinary skill in the art, signature is the integrity information in the encrypted sample. By checking the signature of an encrypted document, it is checking the integrity information included with the biometric sample.

22. Applicant's argument over claims 11 and 24 are not persuasive and the examiner disagrees. Examiner respectfully points out in the above item 18 of the examiner's response to the argument, examiner explains that by the checking the signature of an encrypted document, it is checking the integrity information included with the biometric sample. To a person with ordinary skill in the art, signature is a unique transaction identifier in checking the integrity information included with the biometric sample.

23. Applicant's argument over claims 12 and 25 are not persuasive and the examiner disagrees. Examiner respectfully points out in fig. 416 in fig. 4, "Server signs this data using the server private key". User identification information is the user's biometric data to a person with ordinary skill in the art. By singing the data using the server private key as disclosed in the Gould et al. reference, it is associating user identification information with the private key. Therefore, the Gould et al. reference met the claimed limitation. Also, the examiner respectfully points out in the argument page 9-10, the Applicant argues "...a private key that is provided to a user as required by the claims". Examiner respectfully disagrees since "providing access to a private key in accordance with a result of the comparing step" is not the same as "...a private key that is provided to a user". According to claims 1 and 14, the claim limitation "providing access to a private key..." is broader than Applicant's argument "...a private key that is provided to a user".

24. Applicant's argument on pages 10-11 of Claim rejection under 35 U.S.C. 103 are not persuasive, the examiner disagrees.

First, amended independent claims are addressed in the above 35 USC § 112 rejection new ground rejection using the Gould et al. reference. Therefore, prima facie case of obviousness rejection in view of Gould et al. reference is established.

Second, the examiner reminds the Applicant that rejections over claims 6-8 and 19-21 are 103 obvious rejections, not 102 anticipate rejection. In the first action, the examiner points out that Gould et al. does not specifically show generating pre-enrollment keys and final pre-enrollment key from different individuals and it is common knowledge in the art. Therefore, the examiner takes official notice to illustrate the process of generating pre-enrollment keys and final pre-enrollment key from different individuals by giving an example of a department store credit card issuing scenario to prove this is common knowledge to a person with ordinary skill in the art. The Applicant argues that "This subject matter is explicitly required by the claims and is not required in a department store credit card issuing scenario as described in the Office Action" is not persuasive and it is wrong. Indeed, it is common knowledge in the art and it is required in a department store credit card issuing process in the store.

Third, the Applicant argues that "Gould says nothing whatsoever about an enrollment process... Gould merely states that a biometric template for an employee is typically created when the employee is initially granted access to the system (col 5, lines 28-31", the Applicant contradicted himself with his own statement. If Gould et al. discloses a biometric template for an employee is typically created when the employee

is initially granted access to the system, is this not an enrollment process? Also in steps 308 and 309 in fig. 3 of system set up of the Gould et al. reference, "Establish biometric input for user" and "Associate biometric input and credentials on server" are clearly enrollment process.

25. Applicant's argument on traversing nonstatutory obviousness type double patenting in view of claims 1, 17, 18, 20, 36, 39 and 44 of co-pending application 09/801,468 is acknowledged, it is not persuasive at this time.

First, the newly added claim limitations to independent claims 1, 14 and 27 of the current application are rejected under 35 USC § 112 first paragraphs as applied above.

Second, the limitations "determining whether the request requires authentication" and "database that stores a plurality of biometrics for a respective plurality of users" in the co-pending application are obvious to a person with ordinary skill in the art in comparison with the current application. Although the conflicting claims are not identical, they are not patentably distinct from each other and encompass the same subject matter.

Third, Applicant mentioned the co-pending application claims have been amended and should include even further elements that are not found in the present claims. Therefore, examiner requests a copy of the most current amended claims of the co-pending application. Please note this is nonstatutory **obviousness-type** double patenting rejection. Therefore, more elements added are not necessarily overcome the rejection. They have to be nonobvious in order for the examiner to consider withdrawing the rejection.

Therefore, due to the above reasons, the examiner maintains the double patenting rejection.

Conclusion

26. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-892)

27. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to April Y. Shan whose telephone number is (571) 270-1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

16 February 2007
AYS

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Notice of References Cited	Application/Control No. 10/612,715	Applicant(s)/Patent Under Reexamination SOTO ET AL.	
	Examiner April Y. Shan	Art Unit 2135	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,925,182	08-2005	Epstein, Michael A.	380/277
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

P.O. Box 1450
Alexandria, VA 22313-1450
If Undeliverable Return in Ten Days

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

AN EQUAL OPPORTUNITY EMPLOYER

U.S. OFFICIAL MAIL
PENALTY FOR
PRIVATE USE $300
PITNEY BOWES
02 1A $ 01.35⁰
0004204479 FEB 26 2007
MAILED FROM ZIP CODE 22314

PILL600 221022056 1A05 03 03/01/07
FORWARD TIME EXP RTN TO SEND
:PILLSBURY WINTHROP SHAW PITTMAN LLP
1650 TYSONS BLVD STE 1400
MC LEAN VA 22102-4864

RETURN TO SENDER